REMARKS

In response to the Final Office action of March 3, 2006, applicant asks that all claims be allowed in view of the above amendment to the claims and the following remarks.

Claims 1-6, 8-12, 16-20, 22-25, 27-37, 39-43, 47-51, 53-56, 58-68, 70-74, 78-80, 83-86, and 88-92 are now pending, of which claims 1, 19, 32, 50, 63 and 79 are independent. Claims 1-3, 16-20, 20, 22, 32-34, 47-48, 50-51, 53, 63-65, 78-80, and 83 have been amended. Support for these amendments may be found, for example, in the Specification, page 14, lines 13-31 and page 15, lines 1-31. Claims 7, 13-15, 21, 26, 38, 44-46, 52, 57, 69, 75-77, 81-82, and 87 have been canceled. No new matter has been introduced.

Rejections under 35 U.S.C. 103

Claims 1-92 have been rejected under 35 U.S.C. 103 as being unpatentable over Bin Abdul Rahman (U.S. Publication No. 2002/0184501) in view of Cane (U.S. Patent No. 5,416,840). Applicant has amended claims 1, 19, 22, 50, 63 and 79 to obviate this rejection, and thus requests reconsideration and withdrawal of the rejection of claims 1-6, 8-12, 16-20, 22-25, 27-43, 47-51, 53-56, 58-68, 70-74, 78-80, 82-86, and 88-92. Neither Bin Abdul Rahman, Cane, nor any valid combination of the references describes or suggests the subject matter of the independent claims. For example, neither Bin Abdul Rahman, nor Cane, nor any combination of the two describes or suggests receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier. Nor does Bin Abdul Rahman, Cane, or the proposed combination describe or suggest performing a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system, and comparing results of the first and second mathematical computations, as similarly recited in amended independent claims 1, 19, 32, 50, 63 and 79.

Claims 1-18, 32-49 and 63-78

Independent claim 1, as amended, recites a method for determining whether a client communication system seeking access to a host communication system is authorized to do so.

The method includes receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed on the access password and the client-communication-system-specific identifier. The method also includes accessing, at the host, a password and performing a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system. The method further includes comparing results of the first and second mathematical computations and designating a client communication system as unauthorized based on the comparison results of the first and second mathematical computations where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Bin Abdul Rahman, the primary reference, discloses a method of establishing secure data transmission in a network using an optical media key.[1] In Bin Abdul Rahman, a client application initially accesses encrypted data, such as software data on a CD-ROM, and requests a public key. The client receives the public key and decrypts a digital certificate and token identification information from the data.[2] If the token identification information is determined to be valid, a user digital certificate is created.[3] The server application retrieves a certificate revocation list and verifies the user digital certificate.[4] If a user record associated with the user digital certificate is found, a challenger-response method for password verification is employed. A random challenge value is generated and sent to the client.[5] In the next two steps (step 54 and 55 in Fig. 2), the client generates and sends a response value to the merchant server using a challenged value, the public key, and the user password, and the server analyzes the response value.[6]

Applicant submits that the detailed description of steps number 54 and 55 in Fig. 2 are inconsistent and conflicting in the description and terminology. Consequently, based on the specification, the specific process of steps 54 and 55 appear indeterminate.

---

[1] See Bin Abdul Rahman, Title
[2] See Bin Abdul Rahman, Paragraph [0041]
[3] See Bin Abdul Rahman, Paragraph [0042]
[4] See Bin Abdul Rahman, Paragraph [0043-0044]
[5] See Bin Abdul Rahman, Paragraph [0047]
[6] See Bin Abdul Rahman, Paragraph [0047]

Turning first to steps in the process, and the relevant terminology, paragraph [0047] states (emphasis added) that "a random challenge value is generated by the server application and forwarded to the client application" and "the user password is authenticated at step 51, by the client application generating a response value using the user password, the user private key 21, and the challenged value received from the server application." Paragraph [0047] goes on to state that "the merchant server 4 then computes a value with the same calculation formula using the challenge value sent by the client application... the sever application then compares the challenge value with the user's response value." Paragraph [0048] states that "if the challenge and response values are determined by the server application to be equal at step 55 the client application is provided access." Applicant assumes that references to the "random challenge value," the "challenged value," and the "challenge value" are all intended to reference the same value.

Turning to inconsistency, the third reference above is to a challenge value sent by the client application, as quoted above. The specification does not appear to show or suggest the challenge value is sent from the client application to the server. Rather, the specification appears to state that the random challenge value is sent from the server to the client application, where the client application uses it (described as the challenged value) and other values to generate a response which is sent to the server.

Further, after receiving the response value from the client application the server "then computes a value" and paragraph [0048] states that "the sever application then compares the challenge value with the user's response value...if the challenge and response values are determined by the server application to be equal at step 55 the client application is provided access," as quoted above. Applicant submits that the process, as described, does not appear to make sense. Specifically, the response value is described earlier as generated "using the user password, the user private key, and the challenged value." Thus the response value appears to be inherently not equal to the challenge value since the response value is generated with other values such as the key.

While applicant makes no suggestion as to any specific interpretation as to what is meant by steps 54 and 55, Applicant notes that after receiving the response value, the server application then generates "a value with the same calculation formula" and the "a value" generated in

response to receiving the response value from the client application is not seen to be mentioned again.

As described above, Rahman is seen to teach a method where authentication is carried out by a client generating a response value using a challenge value, a password, and a key, and then sends this value to a server. The server then is seen to make a comparison with the received response value and determine authentication.

Applicant submits that Rahman does not describe or suggest (1) receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier or (2) performing a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system, and comparing results of the first and second mathematical computations, as recited in amended claim 1.

The significance of a client sending both the identifier and results of the computation may be shown by the second mathematical computation. As described in the claim, the second mathematical calculation is performed at the host using a local value (the password retrieved locally at the host) and a value originating at the client (the a client-communication-system-specific identifier). At the host, the received (first) and locally performed (second) mathematical calculations are compared to determine authorization. Thus, by requiring the host accurately receive a value to be compared and an identifier used in the generation of the comparison value, a further degree of security is achieved. In contrast, Rahman is seen to describe the generation and sending of a single value (the response value) from the client to the server.

Cane, the secondary reference in the rejection, discloses a process for unlocking software. The Cane process generates an encrypted password that is sent to the user's computer and using the password, the personal computer decryption device of the user's computer is used to decrypt and "unlock" software.[7] This is also shown in Cane at FIG. 4 (illustrating a flow diagram of a preferred environment in which a software vendor 400 provides encrypted software to a

[7] See Cane at col. 3, lines 28-38 and col. 4, lines 27-36

publishing center 401, which, in turn, provides encryption key and software identifier information to an order center 402, which provides a user 404 with a password to unlock the software after purchase) and col. 5, lines 19-43 (describing the flow between the entities of FIG. 4).

More particularly, Cane's process for unlocking software includes generating a password using a software encryption key and a password key.[8] The particular software encryption key to be used corresponds to the software to be unlocked and is determined by looking up, in the software-key table, the software identifier of the software to be unlocked.[9] The particular password key to be used corresponds to the password key stored on the personal computer decryption device of the computer on which the software to be unlocked resides, and the particular password key is determined by looking up, in the serial number-key table, the hardware identifier stored in the personal computer decryption device.[10] Presumably, the software encryption key is encrypted with the password key. In any event, the encrypted password is sent to the user's computer, and the personal computer decryption device decrypts, using its stored password key, the password, which "recovers" the software encryption key.[11] The software encryption key then is used to decrypt the software.[12]

Applicant's prior response to the Non-Final Office Action pointed out that Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier. The Final Office Action acknowledged this point, noting that the arguments "are persuasive" and withdrawing the then-perused rejection,[13] submitted a new rejection where the above limitation was rejected with a new reference (Bin Abdul Rahman).

Applicant submits that as a consequence of Cane's failure to describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, Cane does not describe or suggest the <u>further limitations</u> of (1)

---

[8] See Cane at col. 6, lines 31-38; col. 7, lines 64-67; col. 4, lines 27-36
[9] See Cane at col. 6, lines 31-34 and col. 4, lines 27-34
[10] See Cane at col. 6, lines 31-34 and col. 4, lines 27-34
[11] See Cane at col. 5, lines 5-7 and col. 6, lines 45-53
[12] See Cane at col. 6, lines 54-58
[13] See Final Office Action, Page 2

receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier or (2) performing a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system, and comparing results of the first and second mathematical computations, as recited in amended claim 1.

For at least these reasons, applicant respectfully requests withdrawal of the rejection of independent claim 1, along with claims 2-6, 8-12, and 16-18 that depend therefrom.

Independent claim 32 recites a computer readable medium or propagated signal having embodied thereon a computer program for identifying an unauthorized client communication system seeking access to a host communication system in a manner corresponding to that of independent claim 1, and independent claim 63 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 32 and 63, along with claims 33-43, 47-49, 64-68, 70-74, and 78 that depend therefrom.

Claims 19-31, 50-62 and 79-92

Independent claim 19 recites a method for handling information about an authorized client communication system. The method includes storing a version of an access password and storing a client-communication-system-specific identifier and results of a first mathematical computation performed, at the client communication system, on the access password and the client-communication-system-specific identifier from the client communication system received from a client. The method also includes performing a second mathematical computation on the stored access password and the retrieved client-communication-system-specific identifier and storing the results of the second mathematical computation when the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 19, along with claims 20, 22-25, and 27-31 that depend therefrom.

Independent claim 50 recites a computer readable medium or propagated signal having embodied thereon a computer program for handling information about an authorized client communication system in a manner corresponding to that of independent claim 19, and independent claim 79 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 50 and 79, along with claims 51, 53-56, 58-62, 83-86, and 88-92 that depend therefrom.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant submits that all claims are in condition for allowance.

No fees are believed due at this time. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 5/3/2006

W. Karl Renner
Reg. No. 41,265

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40332946.doc